FAILURES OF SET IMPLEMENTATION: WHAT IS AMISS?

Pita Jarupunphol and Chris Mitchell

Information Security Group, Royal Holloway, University of London

(P.Jarupunphol@rhul.ac.uk, C.Mitchell@rhul.ac.uk)

Abstract

Although e-commerce provides many benefits to consumers, e.g. convenience, greater choice, lower prices, and more information, there are also a number of barriers restricting its growth. Credit card fraud is currently one of the most serious issues in e-commerce, since it makes consumers reluctant to engage in this alternative method of shopping. Secure Electronic Transaction or SET is arguably the most secure method of payment by credit card over the Internet, and it was purposely designed to address all potential threats to Internet e-commerce transactions. However, SET has not really taken off; implementation issues appear to be the main factor restricting its adoption. For example, complexity of end-user initialisation, transaction speed, and cost of investment all appear to be significant issues. The intention of this paper is to consider the true nature of the SET implementation difficulties and how things might be changed to achieve higher levels of adoption.

Keywords: Electronic Commerce (E-Commerce), Secure Socket Layer (SSL), Secure Electronic Transaction (SET), Transport Layer Security (TLS), e-commerce end-users.

1 Introduction

The emergence of e-commerce provides consumers with an alternative method of payment via the Internet. This reduces the effort and time spent in traditional shopping methods [6]. For example, there is no need for consumers to go to retail premises in order to purchase goods. However, this non face-to-face shopping method also enables fraudsters to exploit the lack of any built-in user authentication facilities within the Internet to perform illegal operations, such as the use of credit card numbers without the consent of the valid cardholder [2]. This threat is accentuated by the fact that the Internet also lacks any built in privacy features, which means that otherwise unprotected credit card numbers sent across the Internet as part of a transaction are prone to interception.

The credit card is the most common method of payment in business-to-consumer (B2C) transactions [20]. In fact, a survey of Internet users conducted by Survey.Net (http://www.survey.net) indicates that more than 50% of Internet users purchase products or services by credit card. Therefore, it is inevitable that the security of credit card numbers is an issue of serious concern to Internet purchasers. Many consumers are afraid of submitting their credit card numbers via the Internet, and also perceive Internet shopping as the riskiest method of payment [15], [19].

2 Overview of e-commerce security requirements

Since e-commerce involves the transfer of a variety of payment-related data over the Internet, there are a number of security requirements for the transaction, including confidentiality, integrity, authentication, authorisation, and non-repudiation [18]. We can summarise these requirements as follows.

Confidentiality – consumer financial information, such as credit card numbers, must not be compromised or intercepted by malicious intruders.

Integrity – all sensitive information transmitted in e-commerce transactions must remain accurate and not be modifiable.

Authentication – e-commerce end-users (consumers and merchants) must be able to verify each others' identities.

Authorisation – consumers and merchants must have appropriate authorisations for the e-commerce transaction.

Non-repudiation – consumers and merchants must not be able to repudiate a properly conducted transaction.

3 End-user security requirements

Consumers would appear to have rather negative perceptions of the security of present-day e-commerce, [15]. Additionally, some merchants are also reluctant to engage in e-commerce. Consumer and merchant concerns arise for a number of reasons, some of which we now consider.

3.1 Lack of authentication for e-commerce participants

As Internet e-commerce is a non-face-to-face shopping method, identity verification of merchants is a concern to potential e-commerce participants. That is, consumers wish to be assured that the merchant that they are dealing with is the genuine party, and not a third party masquerading as a reputable merchant. Merchants, on the other hand, need to verify that the e-consumer is who they claim to be and is not using a borrowed or stolen credit card or credit card number to initiate transactions.

3.2 Lack of confidentiality for payment information

Many consumers are concerned that their credit card numbers will be compromised during data transmission or storage when they are participating in e-commerce. Consumer financial information is potentially an attractive target for intruders since, in some circumstances, it can be used to conduct fraudulent transactions. There is also a risk that the compromise of consumer credit card numbers can damage a merchant's reputation, whether or not the compromise is the fault of the merchant.

3.3 Privacy requirements

Many consumers are not only concerned about the confidentiality, but also the privacy of their financial information. Since the trustworthiness of merchants is one of the most important issues of concern to potential e-commerce consumers, there is a need for consumers' financial information to remain private although it is transmitted to merchant web servers. Merchants also have e-commerce privacy requirements, since they may be reluctant to disclose full details of consumer order information to their banks.

There are several tools and techniques that, at least partly, address consumer fears, including SSL/TLS [[8] and SET [10]. SET is arguably the most secure method of online payment by credit card, and it limits the access that banks and merchants have to sensitive consumer information. However, SET has not really taken off, probably because of implementation issues. The intention of this paper is to further investigate the obstacles to SET adoption.

4 SET and e-commerce

Since e-commerce allows people to place an order via the Internet, there are also several potential security threats associated with it. Online fraud is arguably an issue of concern to all e-commerce participants, including consumers, merchants, and their respective financial institutions. SET, which was invented by Visa (http://www.visa.com) and MasterCard (http://www.mastercard.com), is a method to secure entire e-commerce transactions. SET is arguably able to address several categories of fraud in Internet e-commerce transactions.

4.1 Credit card fraud

SET supports long key lengths for both symmetric and asymmetric encryption, such as triple DES and 1,024-bit RSA, [16], [17]. There is thus no risk of credit card numbers being compromised via interception. In addition, even if unauthorised access to a merchant web server occurs, the confidentiality of consumer payment information will not be endangered since it is encrypted using an acquiring bank public key, i.e. it is not available to the merchant. Thus SET can prevent credit card fraud arising from transmission and storage of sensitive data.

4.2 Merchant fraud

In SET, order and payment information are encrypted separately for specific recipients. That is, merchant public keys are used to encrypt order information and acquiring bank public keys are used to encrypt payment information. Consumers can thus be assured that their credit card numbers will not be compromised by a fraudulent merchant.

In addition, to prevent merchants modifying payment details, e.g. to increase the value of a sale, as part of SET the consumer PC adds a digital signature to all relevant transaction information.

4.3 Consumer fraud

Since the Internet offers no guarantees about the identity of the originator of a transaction, it is difficult for merchants to check whether consumers are using stolen credit card numbers to initiate transactions. In cases where consumers use a stolen credit card to initiate e-commerce transactions, merchants are responsible for 'card not present' transaction charge backs, [12], [20]. In SET, consumers must authenticate themselves to their local PC by entering a password to activate their digital wallet prior to initiating a transaction [16]. The consumer' s PC then transmits completed order form and payment instructions to the merchant. As SET employs digital signatures to authenticate the cardholder PC, merchants can verify the legitimacy of the cardholder. This means that the SET scheme can address consumer fraud deriving from misuse of credit card numbers.

4.4 Internet fraud

The Internet link between customer and merchant may be subject to manipulation by a malicious third party. The use by SET of digital signatures, as mentioned in Section 3.2, prevents this.

5 Criticisms of SET

SET has not really taken off probably primarily because of implementation issues, including low transaction speed, complexity, inflexibility, etc. [15]. Figure 1 analyses causes and effects when implementing SET.

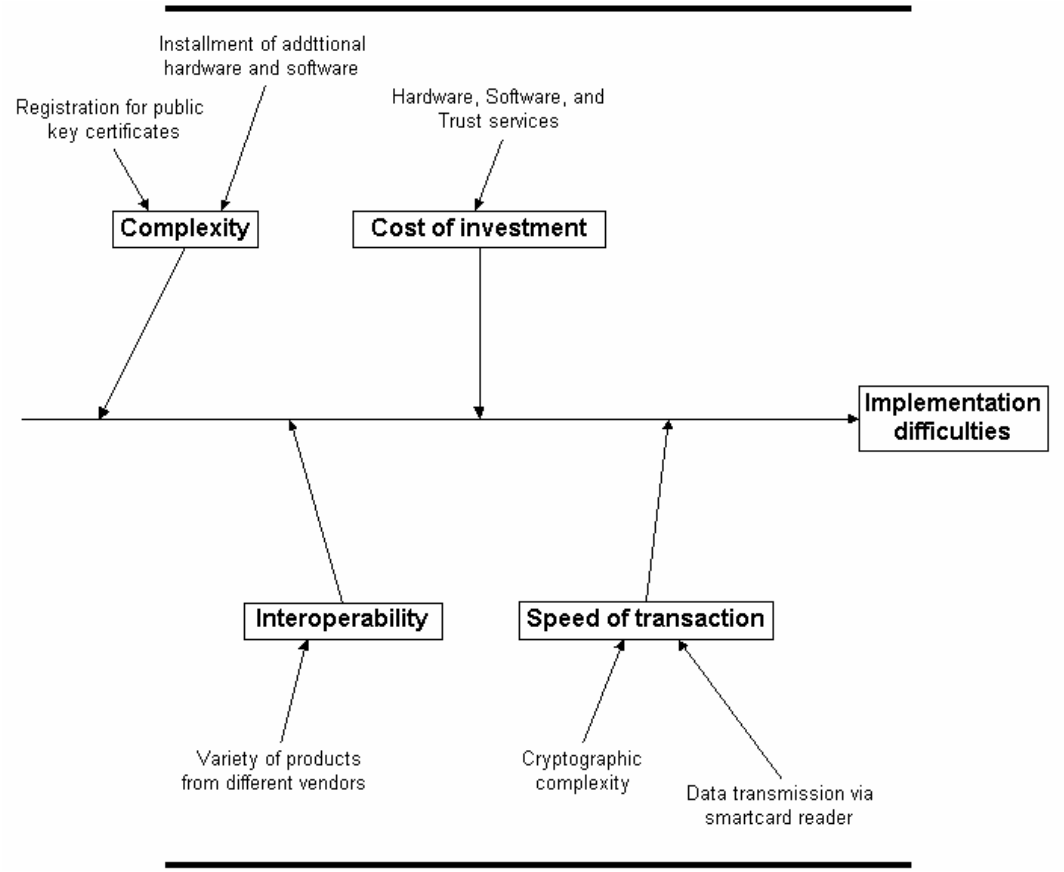

Fig. 1 Causes and effects on SET/EMV implementation

We now focus on possible reasons for these criticisms of SET.

5.1 Getting the right balance

Consumer confidence in e-commerce is arguably a key enabler to its growth. However, recent research indicates that consumers are very concerned about the security of their financial information when making e-commerce transactions

[1], [14]. However, it is an oversimplification to suppose that security should be considered as an overriding issue for the typical user. For many users, a high level of security may not be important; instead providing security at an acceptable level in a less complex way may better meet end-user requirements. The SET developers have designed a very effective security system for e-commerce transactions, but have ignored other important factors. Although a high level of security is necessary where sensitive information, such as credit card numbers, is at risk, other issues, such as ease of use and speed of transactions, are also critical to the end user. This means that developers of e-commerce security systems need to consider ease of implementation and use for e-commerce end-users instead of just providing the highest possible level of protection.

5.2 Lack of end-user participation

It is generally recognised that end-users should play a significant role in the development of new systems. According to Viega et al. [9, p33], "The lack of communication causes developers to make assumptions about the implementation…developers may not have precise knowledge about the environment in which their code will run". Given the complexity of end-user initialisation it is reasonable to assume that there was little or no end-user participation in the development of SET before it was issued to the public. As a result, the SET developers may well have focussed on the end-user security requirements rather than how the system can be readily implemented and operated by end-users.

In order to ensure that the system meets end-user requirements, the developer must involve end-users in the system design process. Prototyping, for example, is one of several software development approaches that facilitates the desired interactions between developers and end-users [3], [11].

5.3 Lack of understanding of consumer Internet skills

Since there are numerous Internet users who may potentially place an order through the Internet, the level of skill of the majority of Internet users is a vitally important factor when designing a payment security scheme.

For the more sophisticated consumers, ordering products via e-commerce may not be difficult. These users can comfortably purchase products or services online. It is reasonable to suppose that such users will understand the benefits of e-commerce. As a consequence, we suppose that the minority of sophisticated Internet users should have no problem with registering for a digital certificate and downloading a digital wallet from a SET software supplier.

By contrast, the less sophisticated majority of Internet users may have some difficulty in searching for the items they wish to purchase, and in placing an e-commerce order. Since participating in e-commerce may already be difficult for such users, the certificate registration and digital wallet installation processes are likely to pose an insurmountable obstacle to use of SET.

Hence, one possible shortcoming in the design and implementation of SET, at least up to the present, is in failing to appreciate what it is reasonable to expect of end-users. Any such system will be doomed to failure if it requires the e-commerce participant to be an 'expert user' in any sense.

5.4 Lack of third party support

As stated earlier, SET addresses all possible threats that might lead to online credit card fraud. Although SET implementation is complex, SET still seems to be the most appropriate scheme for Internet e-commerce security, given that many consumers are still very concerned about the threat of credit card fraud. However, most e-commerce web sites are still using SSL to secure transactions, although SSL was not specifically designed to provide security for Internet e-commerce transactions. Indeed, SSL was designed to provide security purely for a communications link, and hence fails to address many of the security issues for an e-commerce transaction. So, why is SET not used more widely? One reason for the failure of SET to become widely used might be because of inadequate support from governments and other third parties.

One way in which the adoption of SET could be facilitated would be if governments or trade bodies positively encouraged merchants and card issuers to adopt SET, e.g. by requiring its use for their e-business. Furthermore, cooperation with the suppliers of the major Internet browsers, such as Internet Explorer and Netscape Communicator, could be used to make SET implementation much easier for consumers. For example, if the two major Internet browsers contained pre-installed digital wallets supporting SET, then the adoption of SET would be greatly simplified. Figure 2 gives a diagrammatic representation of SET implementation issues.

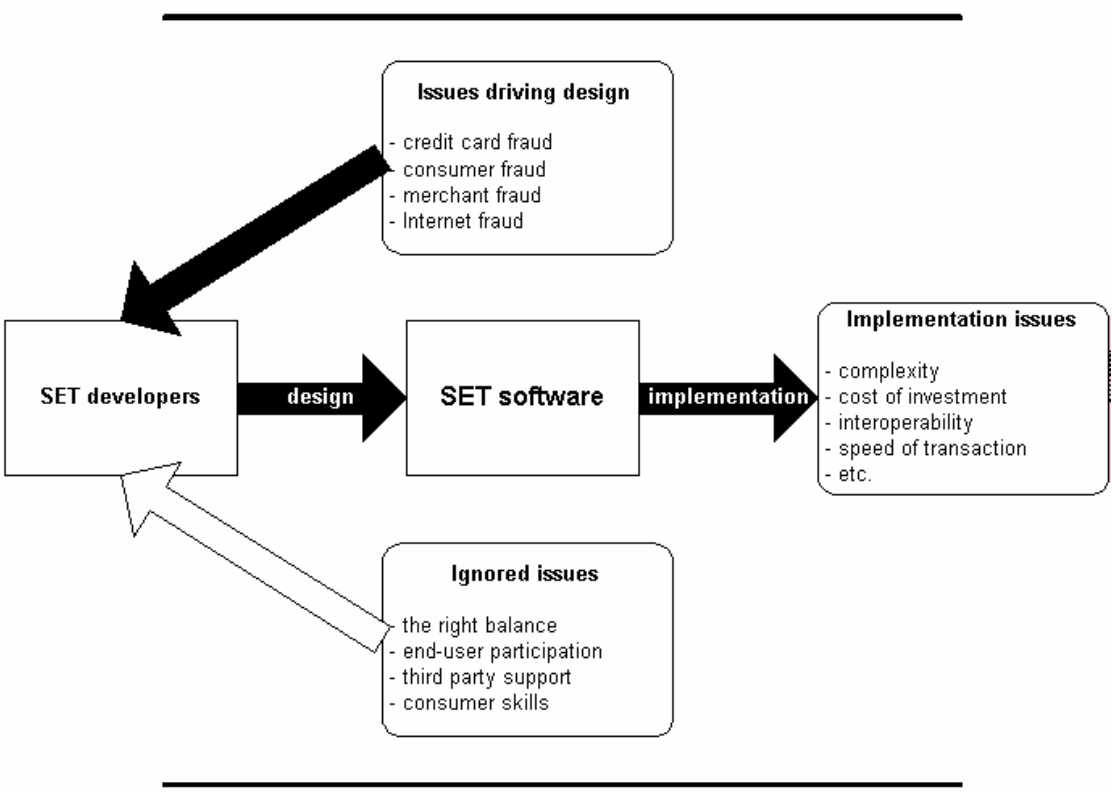

Fig. 2 Reasons behind SET implementation issues

6 Current developments in SET

Several SET extensions have been invented in order to overcome the existing implementation barriers, such as the so-called PIN and Chip extensions, [4], [13]. SET/EMV or EMV/SET, which is the integration of SET technology with the EMV industry standard for chip cards [7], and 3D SET [5], are current examples of attempts by the SET developers to simplify installation and use of SET. We now discuss these two recent developments in more detail.

6.1 SET/EMV or EMV/SET

SET/EMV was invented in order to reduce the complexity of SET end-user initialisation, but retain SET' s security features. In order to participate in SET/EMV, e-commerce consumers need to possess an EMV-compliant debit/credit card and to install a smart card reader at their PC. EMV-compliant Consumer credit cards will communicate with the consumer PC via the smart card reader to support the interactions between consumer PC and Merchant Server necessary to conduct a SET transaction. In SET/EMV, there is no requirement for e-commerce consumers to register for a public key certificate, since the key pair and certificates already contained in the EMV smart card can be used instead. The benefits of SET/EMV include the following.

- Consumers can purchase products or services from any PCs that have a smart card reader and the appropriate software installed.
- Consumers do not need to worry about threats to their private key, since it is no longer stored at the consumer PC.

6.2 3D SET

3D SET [5], which was proposed by Visa, is an alternative version of the SET scheme that builds upon the relationship between three domains in e-commerce transactions, namely the acquirer, issuer, and interoperability domains. Since many of its transaction processes are performed using direct connections between the three domains, 3D SET is able to eliminate some of the SET implementation issues, as follows.

Acquirer Domain – The acquirer domain covers the relationship between the merchant and acquirer. Merchant certificates are held in a secure server, which significantly facilitates the payment process.

Issuer Domain – The issuer domain covers the relationship between the cardholder and the issuer. The cardholder payment functionality is implemented on a secure server. In this case, there is no need for consumers to store certificates on their PC, since the Issuer secure server will provide the security functionality.

Interoperability Domain – The relationship between the acquirer and issuer is supported by the interoperability domain.

7 Conclusions

SET is currently the most effective method to secure online transactions since it meets all the main e-commerce security requirements. However, SET has not been widely adopted for a variety of reasons, including implementation issues. Nevertheless, given that serious e-commerce security issues remain, SET is still of potentially great value in increasing confidence in, and hence adoption of, e-commerce. Various SET modifications and enhancements, including the so-called PIN and Chip extensions, have been introduced to try and facilitate implementation and hence increase adoption of SET. Regardless of the success of these enhancements to SET, the developers of SET and of future systems need to consider carefully why SET has, at least so far, failed to take off. If the lessons from these problems are not acted upon, then future systems will almost certainly face similar problems.

SET adoption and use would clearly benefit from support from governments and other third parties. Such support could range from regulatory support from governments to inclusion of SET functionality in widely used PC software, such as web browsers. At the same time, end users of e-commerce might usefully be encouraged to adopt SET, e.g. by emphasising its benefits, offering financial inducements, or simply facilitating the wider use of smart card readers. Should SET eventually succeed, it could do much to eliminate existing types of credit card fraud, a benefit to all parties, including end users, merchants and banks. Finally, although SET is widely regarded as being 'dead', the fact that various modifications to SET, such as the chip extensions, have recently been introduced, as have variants such as 3D SET, means that the idea of SET lives on, and it remains likely that some kind of SET-like system will eventually be widely adopted.

Acknowledgements: Pita Jarupunphol was sponsored by the Rajabhat Institute of Phuket.

References

[1] Amit Bhatnager, Sanjog Misra, and H. Raghav Rao; On risk, convenience, and Internet shopping behaviour, Communication of the ACM, Vol. 43, Issue. 11, pp98-106, November, 2000.

[2] Anup Ghosh; E-Commerce Security: Weak Links, Best Defences, John Wiley and Sons, New York, 1998.

[3] Barbara McNurlin, and Ralph Sprague; Information Systems Management in Practice 4th, Prentice-Hall, New Jersey, 1998.

[4] Common Chip Extension – Application for SETCo Approval, SETCo.Org, Version 1.0, 1999a.

[5] David Bounie, and Livio Vaninetti; E-Payments: Which Systems in Europe for the Coming Years?, ENST, May, 2001.

[6] David Whiteley; E-Commerce: Strategy, Technologies and Applications, McGraw-Hill, Berkeley, 2000.

[7] EMV '96 Chip Electronic Commerce Specification, EMVCo.Org. Version 1.0, 1999.

[8] Eric Rescorla; SSL and TLS – Designing and Building Secure Systems, Addison-Wesley, Boston, 2001.

[9] John Veiga, Todayoshi Kohno, and Bruce Potter; Trust and mistrust in secure applications, Communication of the ACM, Vol. 44, Issue. 2, pp31-36, November, 2001.

[10] Mark Merkow, Jim Breithaupt, and Ken Wheeler; Building SET Applications for Secure Transactions, John Wiley and Sons, New York, 1998.

[11] Merle Martin; Analysis and Design of Business Information Systems, Prentice-Hall, New Jersey, 1995.

[12] Nick Caunter; The real cost of fraud to e-tailers, Computer Fraud and Security, 2001(8), ppl-17, 2001.

[13] Online PIN Extensions to SET Secure Electronic Transaction, SETCo.Org, Version 1.0, 1999b.

[14] Pita Jarupunphol, and Chris J. Mitchell; Actual and perceived levels of risk in consumer e-commerce. In Proceedings of 2nd International We-B Conference, Edith Cowan University Press, Perth, pp. 207-216, November, 2001.

[15] Pita Jarupunphol, and Chris J. Mitchell; The Future of SET. In Proceedings of UKAIS 2002, Leeds, April, 2002.

[16] SET Secure Electronic Transaction Specification – Book 1: Business Description, SETCo.Org, Version 1.0, 1997a.

[17] SET Secure Electronic Transaction Specification – Book 2: Programmer's Guide, SETCo.Org, Version 1.0, 1997b.

[18] Vesna Hassler; Security Fundamentals for E-Commerce, Artech House, Massachusetts, 2000.

[19] Vivienne Farrell, Ying Leung, and Graham Farrell; A study on consumer fears and trust in Internet based electronic commerce, In Proceedings of 13th International Bled Electronic Commerce Conference, Slovenia, 2000. Available at (http://www.it.swin.edu.au/centres/cicec/ECTrust/Bled2000.pdf)

[20] Winfield Treese, and Lawrence Stewart; Designing Systems for Internet Commerce, Addison-Wesley, Massachusetts, 1998.